CLAIMS

1. An authenticating device comprising:

an authentication processing unit to perform an authentication process with an authenticated device using an authentication key; and

an update key generating unit to generate a new authentication key when the authenticated device does not hold an authentication key to be used in the authentication process by the authentication processing unit, and to generate a new authentication key for updating an authentication key to be used in the authentication process by the authentication processing unit when the authenticated device holds the authentication key but the authentication process with the authenticated device by the authentication processing unit fails,

wherein the authentication processing unit performs the authentication process with the authenticated device again, using the new authentication key generated by the update key generating unit.

2. The authenticating device of claim 1, further comprising a receiving unit to receive a prescribed algorithm identifier and a prescribed encryption key identifier from the authenticated device,

wherein the update key generating unit generates the new authentication key based on the prescribed algorithm identifier and the prescribed encryption key identifier received by the receiving unit,

the authenticating device, further comprising a transmitting unit to transmit the new authentication key generated by the update key generating unit to the authenticated device,

wherein the authentication processing unit performs the authentication process with

the authenticated device again, using the new authentication key transmitted by the transmitting unit.

3. An authenticated device comprising:

a memory unit to store a prescribed algorithm identifier and a prescribed encryption key identifier;

an authentication processing unit to perform an authentication process with an authenticated device using an authentication key;

a transmitting unit to transmit the prescribed algorithm identifier and the prescribed encryption key identifier stored by the memory unit, to the authenticating device when the authentication process with the authenticating device by the authentication processing unit fails; and

a receiving unit to receive from the authenticating device a new authentication key based on the prescribed algorithm identifier and the prescribed encryption key identifier transmitted by the transmitting unit,

wherein the authentication processing unit performs the authentication process with the authenticating device again, using the new authentication key received by the receiving unit.

4. The authenticated device of claim 3,

wherein the receiving unit receives prescribed information from the authenticating device when the authentication process with the authenticating device by the authentication processing unit fails, and

wherein the transmitting unit transmits the prescribed algorithm identifier and the prescribed encryption key identifier stored by the memory unit, when the prescribed

information has been received by the receiving unit.

5. A key updating method comprising:

a first transmitting step to transmit prescribed information from an authenticating device to an authenticated device when an authentication process fails, the authentication process being performed between the authenticated device which stores a prescribed algorithm identifier and a prescribed encryption key identifier, and the authenticating device, using an authentication key;

a first receiving step to receive the prescribed information transmitted from the authenticating device by the first transmitting step, at the authenticated device;

a second transmitting step to transmit, from the authenticated device to the authenticating device, the prescribed algorithm identifier and the prescribed encryption key identifier stored, after the prescribed information is received by the first receiving step;

a second receiving step to receive the prescribed algorithm identifier and the prescribed encryption key identifier transmitted by the second transmitting step, at the authenticating device;

a generating step to generate a new authentication key based on the prescribed algorithm identifier and the prescribed encryption key identifier received by the second receiving step, at the authenticating device;

a third transmitting step to transmit the new authentication key generated by the generating step to the authenticated device;

a third receiving step to receive the new authentication key transmitted by the third transmitting step, at the authenticated device;

a key updating step to execute a key update using the new authentication key received by the third receiving step, as an update key to perform the authentication process between

the authenticated device and the authenticating device;

a step to generate and transmit an update confirmation data to the authenticating device; and

a step to receive and check the update confirmation data.

6. A key updating method comprising:

transmitting prescribed information from an authenticating device to an authenticated device when an authentication process fails, the authentication process being performed between the authenticated device which stores a prescribed algorithm identifier and a prescribed encryption key identifier, and the authenticating device, using an authentication key;

receiving the prescribed information transmitted from the authenticating device, at the authenticated device;

transmitting from the authenticated device to the authenticating device, the prescribed algorithm identifier and the prescribed encryption key identifier stored, after the prescribed information is received;

receiving the prescribed algorithm identifier and the prescribed encryption key identifier transmitted at the authenticating device;

generating a new authentication key, based on the prescribed algorithm identifier and the prescribed encryption key identifier received, at the authenticating device;

transmitting the new authentication key generated to the authenticated device;

receiving the new authentication key transmitted at the authenticated device;

executing a key update using the new authentication key received, as an update key to perform the authentication process between the authenticated device and the authenticating device;

generating and transmitting an update confirmation data to the authenticating device; and

receiving and checking the update confirmation data.

5